CLAIMS

What is claimed is:

1   1.   An apparatus comprising:

2   a first storage to store a platform identifier unique to a platform;

3   a second storage to store an authentication identifier, the authentication

4   identifier being provided by an authentication vendor using the platform

5   identifier, a platform private key, and an authentication private key; and

6   a signature generator to generate a digital signature for data using the

7   platform identifier and the authentication identifier.

1   2.   The apparatus of claim 1 wherein the signature generator comprises:

2   a platform-specific transformer to transform the authentication identifier

3   using the platform identifier to output an encrypted platform private key; and

4   a decryptor coupled to the platform-specific transformer to decrypt the

5   encrypted platform private key to generate the platform private key using an

6   authentication public key, the authentication public key being provided by the

7   authentication vendor.

1   3.   The apparatus of claim 2 wherein the signature generator further

2   comprises:

3   a signer coupled to the decryptor to sign the data using the platform

4   private key, the platform private key being transparent to the platform.

1   4.   The apparatus of claim 2 wherein the platform-specific transformer

2   comprises:

3   an Exclusive OR (XOR) device to perform an XOR function on the

4   platform identifier and the authentication identifier.

1   5.   The apparatus of claim 2 wherein the platform-specific transformer

2   comprises:

3   a decryptor to decrypt the authentication identifier using a symmetric

4   encryption/decryption key generated from the platform identifier.

1   6.   The apparatus of claim 2 wherein the authentication identifier is

2   generated by a platform-specific reverse transformer which transforms the

3   encrypted platform private key using the platform identifier, the encrypted

4   platform private key being encrypted from the platform private key using the

5   authentication private key.

1   7.   The apparatus of claim 6 wherein the platform-specific reverse

2   transformer comprises an Exclusive OR (XOR) device to perform an XOR

3   function on the encrypted platform private key using the platform identifier.

20

1 8. The apparatus of claim 4 wherein the platform identifier is a unique,

2 serially uncorrelated bit stream.

.1 9. The apparatus of claim 6 wherein the platform-specific reverse

2 transformer comprises an encryptor to encrypt the encrypted platform private

3 key using a symmetric encryption/decryption key generated from the platform

4 identifier.

1 10. The apparatus of claim 1 wherein the platform identifier is installed in the

2 first storage in a protected environment.

1 11. The apparatus of claim 10 wherein the protected environment is a

2 system management basic input/output system table.

1 12. The apparatus of claim 4 wherein the platform-specific transformer

2 further comprises:

3 a reporting device to report the platform identifier to generate a tracked

4 platform identifier.

1 13. The apparatus of claim 1 wherein the platform identifier is a processor

2 serial number retrieved from a processor.

1 14. An apparatus comprising:

2   an encryptor to encrypt a platform private key using an authentication

3   private key to generate an encrypted platform private key, the platform private

4   key being provided by a platform; and

5   a platform-specific reverse transformer to transform the encrypted

6   platform private key to generate an authentication identifier using a platform

7   identifier unique to the platform, the authentication identifier being provided to

8   the platform to generate a digital signature.

1   15.   The apparatus of claim 14 wherein the platform-specific reverse

2   transformer comprises:

3   an Exclusive OR (XOR) device to perform an XOR function on the

4   encrypted platform private key and the platform identifier to generate the

5   authentication identifier.

1   16.   The apparatus of claim 15 wherein the platform identifier is a unique,

2   serially uncorrelated bit stream.

1   17.   The apparatus of claim 14 wherein the platform-specific reverse

2   transformer comprises an encryptor to encrypt the encrypted platform private

3   key using a symmetric encryption/decryption key generated by the platform

4   identifier.

1   18.   A method comprising:

22

2   storing a platform identifier unique to a platform and an authentication

3   identifier in first and second storages, respectively, the authentication identifier

4   being provided by an authentication vendor using the platform identifier, a

5   platform private key, and an authentication private key; and

6   generating a digital signature for data using the platform identifier and

7   the authentication identifier.

1   19.   The method of claim 18 wherein generating digital signature comprises:

2   transforming the authentication identifier using the platform identifier to

3   output an encrypted platform private key; and

4   decrypting the encrypted platform private key to generate the platform

5   private key using an authentication public key provided by the authentication

6   vendor.

1   20.   The method of claim 19 wherein generating the digital signature further

2   comprises:

3   signing the data using the platform private key, the platform private key

4   being transparent to the platform.

1   21.   The method of claim 19 wherein transforming the authentication

2   identifier comprises:

23

3   performing an Exclusive OR (XOR) function on the platform identifier

4   and the authentication identifier.

1   22.   The method of claim 19 wherein transforming the authentication

2   identifier comprises:

3   decrypting the authentication identifier using a symmetric

4   encryption/decryption key generated from the platform identifier.

1   23.   The method of claim 19 wherein the authentication identifier is

2   generated by transforming the encrypted private key using the platform

3   identifier, the encrypted private key being encrypted from the platform private

4   key using an authentication private key.

1   24.   The method of claim 23 wherein transforming the encrypted private key

2   using the platform identifier comprises performing an XOR function on the

3   encrypted platform private key and the platform identifier.

1   25.   The method of claim 21 wherein the platform identifier is a unique,

2   serially uncorrelated bit stream.

1   26.   The method of claim 23 wherein transforming the encrypted private key

2   comprises encrypting the encrypted private key using a symmetric

3   encryption/decryption key generated from the platform identifier.

24

1   27.   The method of claim 18 wherein storing the platform identifier comprises

2   installing the platform identifier in a protected environment.

1   28.   The method of claim 27 wherein the protected environment is a system

2   management basic input/output system table.

1   29.   The method of claim 21 wherein transforming the authentication

2   identifier further comprises:

3   reporting the platform identifier to report a tracked platform identifier.

1   30.   The method of claim 18 wherein the platform identifier is a processor

2   serial number retrieved from a processor.

1   31.   A method comprising:

2   encrypting a platform private key using an authentication private key to

3   generate an encrypted platform private key, the platform private key being

4   provided by a platform; and

5   transforming the encrypted platform private key to generate an

6   authentication identifier using a platform identifier unique to the platform.

1   32.   The method claim 31 wherein transforming the encrypted platform

2   private key comprises:

3   performing an Exclusive OR (XOR) function on the encrypted platform

4   private key and the platform identifier to generate the authentication identifier.

1   33.   The method of claim 32 wherein the platform identifier is a unique,

2   serially uncorrelated bit stream.

1   34.   The method of claim 31 wherein transforming the encrypted platform

2   private key comprises encrypting the encrypted platform private key using a

3   symmetric encryption/decryption key generated by the platform identifier.

1   35.   A computer program product comprising:

2   a machine readable medium having computer program code therein, the

3   computer program product comprising:

4   computer readable program code for storing a platform identifier unique

5   to a platform and an authentication identifier in first and second storages,

6   respectively, the authentication identifier being provided by an authentication

7   vendor using the platform identifier, a platform private key, and an

8   authentication private key; and

9   computer readable program code for generating a digital signature for

10   data using the platform identifier and the authentication identifier.

1   36.   The computer program product of claim 35 wherein the computer

2   readable program code for generating digital signature comprises:

26

3   computer readable program code for transforming the authentication

4   identifier using the platform identifier to output an encrypted platform private .

5   key; and

6   computer readable program code for decrypting the encrypted platform

7   private key to generate the platform private key using an authentication public

8   key provided by the authentication vendor.

1   37.   The computer program product of claim 36 wherein the computer

2   readable program code for generating the digital signature further comprises:

3   computer readable program code for signing the data using the platform

4   private key, the platform private key being transparent to the platform.

1   38.   The computer program product of claim 36 wherein a computer readable

2   program code for transforming the authentication identifier comprises:

3   computer readable program code for performing an Exclusive OR (XOR)

4   function on the platform identifier and the authentication identifier.

1   39.   The computer program product of claim 36 wherein a computer readable

2   program code for transforming the authentication identifier comprises:

3   computer readable program code for decrypting the authentication

4   identifier using a symmetric encryption/decryption key generated from the

5   platform identifier.

1   40.   The computer program product of claim 36 wherein the authentication

2   identifier is generated by a computer readable program code for transforming

3   the encrypted private key using the platform identifier, the encrypted private key

4   being encrypted from the platform private key using an authentication private

5   key.

1   41.   The computer program product of claim 40 wherein a computer readable

2   program code for transforming the encrypted private key and the platform

3   identifier comprises performing an XOR function on the encrypted platform

4   private key and the platform identifier.

1   42.   The computer program product of claim 38 wherein the platform

2   identifier is a unique, serially uncorrelated bit stream.

1   43.   The computer program product of claim 40 wherein a computer readable

2   program code for transforming the encrypted private key comprises a computer

3   readable program code for encrypting the encrypted private key using a

4   symmetric encryption/decryption key generated from the platform identifier.

1   44.   The computer program product of claim 35 wherein the computer

2   readable program code for storing the platform identifier comprises computer

3   readable program code for installing the platform identifier in a protected

4   environment.

1   45.   The computer program product of claim 44 wherein the protected

2   environment is a system management basic input/output system table.

1   46.   The computer program product of claim 38 wherein a computer readable

2   program code for transforming the authentication identifier further comprises:

3   computer readable program code for reporting the platform identifier to

4   generate a tracked platform identifier.

1   47.   The computer program product of claim 35 wherein the platform

2   identifier is a processor serial number retrieved from a processor.

1   48.   A computer program product comprising:

2   a machine readable medium having computer program code therein, the

3   computer program product comprising:

4   computer readable program code for encrypting a platform private key

5   using an authentication private key to generate an encrypted platform private

6   key, the platform private key being provided by a platform; and

7   computer readable program code for transforming the encrypted

8   platform private key to generate an authentication identifier using a platform

9   identifier unique to the platform.

1   49.   The computer program product claim of 48 wherein a computer readable

2   program code for transforming the encrypted platform private key comprises:

3   computer readable program code for performing an Exclusive OR (XOR)

4   function on the encrypted platform private key and the platform identifier to

5   generate the authentication identifier.

1   50.   The computer program product of claim 49 wherein the platform

2   identifier is a unique, serially uncorrelated bit stream.

1   51.   The computer program product of claim 48 wherein the computer

2   readable program code for transforming the encrypted platform private key

3   comprises computer readable program code for encrypting the encrypted

4   platform private key using a symmetric encryption/decryption key generated by

5   the platform identifier.

1   52.   A system comprising:

2   a platform having a unique platform identifier (ID); and

3   a digital signature system coupled to the platform to authenticate data,

4   the digital signature system comprising:

5   a first storage to store the platform identifier;

6   a second storage to store an authentication identifier, the authentication

7   identifier being provided by an authentication vendor using the platform

8   identifier, a platform private key, and an authentication private key; and

9   a signature generator to generate a digital signature for data using the

10   platform identifier and the authentication identifier.

1   53.   The system of claim 52 wherein the signature generator comprises:

2   a platform-specific transformer to transform the authentication identifier

3   using the platform identifier to output an encrypted platform private key; and

4   a decryptor coupled to the platform-specific transformer to decrypt the

5   encrypted platform private key to generate the platform private key using an

6   authentication public key, the authentication public key being provided by the

7   authentication vendor.

1   54.   The system of claim 53 wherein the signature generator further

2   comprises:

3   a signer coupled to the decryptor to sign the data using the platform

4   private key, the platform private key being transparent to the platform.

1   55.   The system of claim 53 wherein the platform-specific transformer

2   comprises:

3   an Exclusive OR (XOR) device to perform an XOR function on the

4   platform identifier and the authentication identifier.

1   56.   The system of claim 53 wherein the platform-specific transformer

2   comprises:

3   a decryptor to decrypt the authentication identifier using a symmetric

4   encryption/decryption key generated from the platform identifier.

1   57.   The system of claim 53 wherein the authentication identifier is generated

2   by a platform-specific reverse transformer which transforms the encrypted

3   platform private key and the platform identifier, the encrypted platform private

4   key being encrypted from the platform private key using the authentication

5   private key.

1   58.   The system of claim 57 wherein the platform-specific reverse

2   transformer comprises an Exclusive OR (XOR) device to perform an XOR

3   function on the encrypted platform private key and the platform identifier.

1   59.   The system of claim 55 wherein the platform identifier is a unique,

2   serially uncorrelated bit stream.

1   60.   The system of claim 57 wherein the platform-specific reverse

2   transformer comprises an encryptor to encrypt the encrypted platform private

3   key using a symmetric encryption/decryption key generated from the platform

4   identifier.

1   61.   The system of claim 52 wherein the platform identifier is installed in the

2   first storage in a protected environment.

1   62.   The system of claim 61 wherein the protected environment is a system

2   management basic input/output system table.

1   63.   The system of claim 55 wherein the platform-specific transformer further

2   comprises:

3   a reporting device to report the platform identifier to generate a tracked

4   platform identifier.

1   64.   The system of claim 52 wherein the platform identifier is a processor

2   serial number retrieved from a processor.

1   65.   A system comprising:

2   a digital signature system;

3   an authentication identifier generator coupled to the digital signature

4   system, the authentication identifier generator comprising:

5   an encryptor to encrypt a platform private key using an authentication

6   private key to generate an encrypted platform private key, the platform private

7   key being provided by a platform; and

8   a platform-specific reverse transformer to transform the encrypted

9   platform private key to generate an authentication identifier using a platform

10   identifier unique to the platform, the authentication identifier being provided to

11   the platform to generate a digital signature.

1   66.   The system of claim 65 wherein the platform-specific reverse

2   transformer comprises:

3   an Exclusive OR (XOR) device to perform an XOR function on the

4   encrypted platform private key and the platform identifier to generate the

5   authentication identifier.

1   67.   The system of claim 66 wherein the platform identifier is a unique,

2   serially uncorrelated bit stream.

1   68.   The of system claim 65 wherein the transform-specific reverse

2   transformer comprises an encryptor to encrypt the encrypted platform private

3   key using a symmetric encryption/decryption key generated by the platform

4   identifier.

5   a first storage to store a platform identifier unique to a platform;

6   a second storage to store an authentication identifier, the authentication

7   identifier being provided by an authentication vendor using the platform

8   identifier, a platform private key, and an authentication private key; and

9   a signature generator to generate a digital signature for data using the

10   platform identifier and the authentication identifier.